
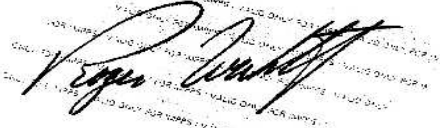



# KANSAS DEPARTMENT OF CORRECTIONS

	<b>INTERNAL MANAGEMENT POLICY AND PROCEDURE</b>	<b>SECTION NUMBER</b>  <b>05-172</b>	<b>PAGE NUMBER</b>  <b>1 of 13</b>
		<b>SUBJECT:</b>  <b>INFORMATION TECHNOLOGY AND RECORDS: KCJIS Network Policy</b>	
<b>Approved By:</b>  <b>Secretary of Corrections</b>		<b>Original Date Issued:</b> <b>07-21-99</b>	
		<b>Current Amendment Effective:</b> <b>08-07-04</b>	
		<b>Replaces Amendment Issued:</b> <b>05-21-01</b>	
<b>Reissued By:</b>  <b>Policy &amp; Procedure Coordinator</b>		The substantive content of this IMPP has been reissued per the appropriate provisions of IMPP 01-101. The only modifications within the reissue of this document concern technical revisions of a non substantive nature. <b>Date Reissued:</b> <b>09-19-11</b>	

## POLICY

The Department of Corrections shall establish and maintain a system of network and physical security consistent with the requirements of the Federal Bureau of Investigation, The Kansas Highway Patrol, CJIS Advisory Board, and the Kansas Bureau of Investigation (KBI) to ensure that access to or modification of KCJIS sensitive data shall be made only by authorized users. Users accessing the system shall be uniquely identified by means of a token issued by the KBI through designated departmental staff. All personnel with any level of KCJIS access shall be trained on privacy and security issues regarding the use of information obtained from the system. All KCJIS equipment, including MDTs and tokens, and systems use are limited to the primary mission of the Department.

## DEFINITIONS

Agency TAC: The Central Office position appointed by the Secretary of Corrections to act as the main point of contact between the Department and the KBI/KHP.

Authorized Users: KDOC personnel who have been approved by the Agency TAC and trained as required on privacy and security issues regarding use of information from the KCJIS system.

Certificate: Person, program or process that can vouch for the identity of a public or private key, by using a cryptographic method to sign certificates. Messages automatically passed from one computer user to another, often through computer networks.

Computer Network: A collection of computers that are physically and logically connected together to exchange information.

Control Terminal Officer (CTO): The Kansas Highway Patrol (KHP) position designated to ensure that CJIS standards, audit standards, and personnel training standards are met for accurate and up-to-date records and dissemination of the same.

Criminal Justice Information System (CJIS): Criminal Justice Information System Integrated information system managed by the Federal Bureau of Investigation.

Destroyed: For the purposes of this IMPP, destruction of information from the KCJIS network means that it will be either shredded or burned.

Dial-in Access: Any access to an interface agency's KCJIS network that provides KCJIS data over public switched circuits on a continuous or temporary basis.

Disabled: For the purposes of this policy, this term means that the modem is turned off and disengaged from the power source.

Encryption: The process of scrambling information in a pre-determined way so that it is unintelligible to anyone who does not know how to unscramble it.

Enterprise IT Security Officer (ESO): The Central Office position appointed by the Information Resource Manager III to oversee the technical management of the network.

Firewall: Hardware and software that secure a site (or internal network) from an external network by examining traffic and imposing access restrictions.

Full Access Operator: Persons whose responsibilities include making entries, modifications, cancels and clears into the NCIC databases  
The Internet: The internet is the largest computer network in the world. It is a three level hierarchy composed of backbone networks (e.g.:ARPAnet, NSFNet, MILNet), mid-level networks, and sub networks. These include commercial (.com or .co) , university (.ac or .edu) and other research networks (.org, .net) and military (.mil) networks and span many different physical networks around the world with various protocols including the Internet Protocol.

Internet: A group of interconnected subnets composed of and with connectivity to The Internet, extranets, and intranets.

Kansas Criminal Justice Information System (KCJIS): A network linking Kansas Criminal Justice Information systems and other national criminal justice networks.

KCJIS Data: Any data any/or images transmitted through the KCJIS network.

KCJIS Sensitive Data: KCJIS data that cannot be disclosed to the public.

KDOC Personnel: For the purposes of this IMPP, any full-time, part-time, temporary, volunteer, contract personnel or anyone else working for the Department.

Law Enforcement Officers: Includes police officers, deputy sheriffs, railroad and campus police, corrections officers and special enforcement officers..

LAN: A local area network. A network in which all of the computers are physically connected to short segments of Ethernet, or token ring, or are connected to the same network hub.

Less Than Full Access Operator: A person whose responsibilities only include inquiry capabilities to one or more components of the NCIC system.

Mobile Data Terminal (MDT): A laptop computer specifically equipped to access the KCJIS network via RF. May also be referred to as mobile computer device or mobile data computer.

Mnemonic: A nine-character internal state routing address, comprised of alpha and numeric characters that identify a device connected to the KCJIS network.

Modem: A device that converts the digital communications of a computer into analog signals that can be carried over a regular telephone line. The term modem in this policy is designated to be a generic term to include analog modems, digital Data Service Units (DSU's), and Channel Service Units (CSU's).

National Crime Information Center (NCIC): A series of databases managed by the Federal Bureau of Investigation.

Network: An internal or external series of devices physically and/or logically connected together to exchange information.

Network Security: Network security includes the physical/electrical links between the desktop and client and the host computer. This responsibility is generally split between agencies - with the user agency and DISC performing part of the functions.

NCIC Full Access Operator: A KCJIS user whose NCIC access allows any NCIC function to be performed included making entries, modifications, cancels, and clears into NCIC databases.

NCIC Less-Than-Full-Access Operator: A KCJIS user whose NCIC access is limited to query functions only.

NCIC Practitioner: An NCIC system user who receives, contributes, or benefits from the NCIC/State system, but does not actually operate a terminal. There are two categories of NCIC practitioners: Law enforcement officers and all other criminal justice employees.

Other Criminal Justice Employees: Includes, but is not necessarily limited to, records clerks, officers of the court, and prosecutors.

Router: An intelligent inter-network connectivity device that routes using logical and physical addressing to connect two or more logically separate networks.

Schematic: A drawing of how a computer network is designed, including all devices and networks that are connected to the agency's local network.

Secure KCJIS: A TCP/IP dedicated network isolated from the open CJIS, open KANWIN, and the Internet by a secured network firewall.

Severe Misdemeanor: Include but are not limited to Aa conviction or diversion of a misdemeanor involving a domestic battery, as an adult or a juvenile, whether or not expunged;. Aa conviction of Driving Under the Influence (or comparable law regarding driving while intoxicated) in the past twenty-four (24) months, as an adult or juvenile;. a conviction of a misdemeanor involving drug use or possession in the past sixty (60) months, as an adult or juvenile.

Terminal Access Control (TAC): A facility/parole office position responsible for ensuring that CJIS/KCJIS policies are enforced at the facility/parole office where they work.

Token: A small item, such as a plastic "smart card", given to each authorized system user that must be used to gain access to the system.

Unauthorized Use/ Access: Exceeding the authorized level of access or use willfully, fraudulently and without authorization gaining or attempting to gain access to any computer, computer system, computer network, or to any computer software, program, documentation, data or property contained in any computer, computer system or computer network.

User: Individual or organizational unit that is authorized to use IT resources.

## **PROCEDURES**

### **I. Network Security**

- A. Access to or modification of the KCJIS sensitive data shall be made only by authorized users.
- B. Each user accessing the system through the KBI KCJIS firewall shall be uniquely identified by means of a token issued by KBI through the Agency TAC.
  - 1. Each workstation accessing the system shall have a unique mnemonic and a valid certificate.
  - 2. Each user shall create his or her own unique Personal Identification Number (PIN).
    - a.(1) The PIN shall not be disclosed to any other individual regardless of the entity or situation.
  - 3. Tokens shall be used only by authorized system users on departmental equipment.
- C. Criminal History Records Information (CHRI) that, by law or official rule, may be disclosed to the public shall not require encryption.

- D. Dial in access to the secure the CJIS router is not permitted by any KDOC personnel.
- E. The KDOC facility network may be comprised of open local area network (WAN)(LAN), closed LAN and regional metropolitan area network (MAN).
  - 1. Access to the facility external, closed LAN shall be limited at the facility firewall and through MS Exchange server administration.
  - 2. Data shall be encrypted on the open LAN at all facilities and parole offices.
    - a. No direct external access shall be allowed into the general open LAN. Dial-in access is permitted to the open KDOC KCJIS network via the regional MANs via a facility RAS server.
- F. No KDOC facility/parole office shall directly access the DISC firewall except for the Central Office.
  - 1. Requests for exceptions shall be addressed in writing to the Agency TAC and Network Security Officer/Enterprise IT Security Officer (NSOESO) for review and approval.
- G. Facilities/parole offices shall provide adequate protection to their devices accessing KCJIS.
  - 1. The program and procedure for providing security shall have been approved by the Network Security Officer/Enterprise IT Security Officer. All regional NOC's shall have a firewall that meets or exceeds the requirements of the KCJIS 's Network Security Policy.
- H. All requests for connection to the KCJIS network shall include a network schematic, a description of how the site meets the relevant policies herein and the level of connection requested.
  - 1. All additional requests for equipment accessing KCJIS shall include a new schematic.
    - a. Such request shall be submitted to the Agency TAC and NSOESO for review and approval.
    - b. After approval, the Agency TAC shall forward the request and attachments to the ASTRA Board in care of the KHP-CJIS Unit.
  - 2. The facility/parole office TAC IT support staff shall each year, on June 30 and December 31, submit to the NSOESO a schematic including internetworking updates and/or significant changes to the network.
    - a. Additional or replacement routers and servers shall be identified to include:
      - (1) RAM size;
      - (2) HD size;
      - (3) Volume name;
      - (4) IP address; and,
      - (5) The number of processors.
    - b. The standard format for schematic design shown in Attachment A, Network Schematic shall be used.
    - c. In no case shall facilities or parole offices submit schematics directly to the KBI/KHP.

- I. All KCJIS data transmitted over wireless links shall be protected with CJIS Security Policy approved encryption, except as noted below:
  - 1. With the exception of FBI Intelligence or criminal history record information, CJIS information transmitted via an RF link to a receiving mobile data computer shall be protected by at least two different operations of data manipulation to ensure CJIS data has been altered from its original clear text format. This includes NCIC hot file information, including any NCIC gang file information, NCIC protection order information and NCIC sexual offender information that is received back to a mobile data computer as a result of an NCIC Query Wanted or Query Vehicle request.
    - a. Any FBI intelligence information or criminal history record information transmitted via an RF link to a receiving mobile data computer shall be protected by a minimum of 56 bit key encryption. This includes information received as a result of a direct query to the NCIC gang files, NCIC protection order files and NCIC sexual offender files.
  - 2. NCIC III detail information shall not be sent to a mobile data computer under any circumstances.
    - a. Criminal history information disclosable to the public by law or official rule does not require encryption.
- K. Internet access via an MDT is authorized only in accordance with IMPP 05-121.
- L. All backups or other copies of KCJIS information shall be protected to preclude unauthorized access to the data when removed from the secured physical location.
  - 1. The programs and procedures for ensuring adequate protection shall have been approved by the ESO.
  - 2. All Criminal History Records Information (CHRI) must be protected from unauthorized dissemination.
  - 3. Dissemination of CHRI is authorized only to other criminal justice administration agencies once a need to know has been verified and it has been verified that the requesting individual is a criminal justice employee.
    - a. However, as secondary dissemination of CHRI is authorized only to other criminal justice employees, they would have authorized access through their own agency and there is no need for them to request dissemination from KDOC.
    - b. Whenever a copy of any CHRI is made, it must be recorded in a secondary dissemination log maintained in the offender record.
    - c. Secondary dissemination logs shall be maintained in the offender record for no less than 3 years after the date of the dissemination.

## **II. Personnel Security Policies**

- A. The Kansas Department of Corrections shall be responsible for the enforcement of KCJIS policies. Personnel covered by these policies include: full-time; part-time; temporary; volunteer; and, contract personnel who have access to the KCJIS network.
  - 1. Applicants for positions accessing KCJIS systems shall be disqualified for further consideration for employment if:
    - a. The applicant has ever been convicted of a felony as an adult, or juvenile, whether or not the record has been expunged; or,

- b. The applicant has ever been convicted of a severe misdemeanor.
  - (1) Any requests for exemptions on misdemeanors shall be made in writing to the Agency TAC.
  - (2) The Agency TAC shall then contact the Control Terminal Officer (CTO) and request an exemption to access the KCJIS network.
- 2. Before access authorization is granted a background check shall be conducted by the Agency TAC. The check shall, at a minimum, include:
  - a. Local name-based check for criminal history record information;
  - b. State and Federal name and fingerprint check for criminal history record information; and,
  - c. Local and Federal warrant check.
- 3. All personnel granted access to the KCJIS network should be at least 18 years of age.
- 4. Personnel who violate any portion of this KCJIS policy are subject to disciplinary procedures outlined in IMPP 02-120.
  - a. Failure to comply with all provisions of this policy may be grounds for termination.
- 5. Employees with KCJIS access whose job assignment no longer requires KCJIS access shall:
  - a. Prior to the end of their last duty shift, return their Security ID Token to the facility/parole office TAC or designee;

### **III. Physical Security Policies**

- A. A. Each facility/parole office shall ensure that the computer site and any related KCJIS equipment shall have adequate security to protect against unauthorized person(s) from gaining access to the computer, network and/or data accessing KCJIS.
  - 1. KCJIS operators using MDTs shall log off KCJIS and the lap top as soon as the requested information is received or any time the operator is not in direct control of the vehicle.
  - 2. The safe operation of the vehicle is an employee's primary responsibility. Use of the MDT is always of secondary importance. Vehicle operators shall not use the MDT simultaneously with vehicle operation.
  - 2.
  - 3. The MDT screen display shall be secured so that unauthorized persons cannot view it.
    - a. Laptop screens shall be closed when the operator is out of the car for extended periods or when the system is not in active use.
  - 4. No unauthorized software or hardware shall be placed on any MDT without prior approval in writing from the Agency Tac and Enterprise IT Security Officer.
    - a. All KCJIS equipment, including MDT's, shall have departmental designated virus scan programs installed and shall use this program to scan any floppy discs used on the MDT system.

- B. The Agency TAC shall be notified immediately within 1 work day upon determination that any equipment accessing KCJIS is lost or stolen.
1. Information that must be related in the notification to the Agency TAC includes:
    - a. The name and title of the person reporting the loss or theft;
    - b. The person's return telephone number;
    - c. A description of the lost or stolen equipment;
    - d. In the case of Secure ID tokens, the name of the holder of the token;
    - e. The location and the time the equipment was last seen; and,
    - f. Information on attempts to locate/recover the equipment.
- C. The TAC shall notify the KBI Help Desk immediately of the lost or stolen equipment.

#### **IV. Technical Policies**

- A. It is the responsibility of the facility/parole office to ensure that no KCJIS sensitive data is allowed to leave the site without prior approval of the records officer for the facility/parole office and without proper documentation of dissemination, per IMPP 05-101.
1. A KDOC Employees Awareness Statement (Attachment B, Form #05-172-001) shall be in place prior to staff from any other agency/company being allowed access to KCJIS sensitive data.
  2. Each facility/parole office records officer shall maintain, for one three years, a secondary dissemination log of KCJIS sensitive data that has left the site.
  3. The log shall be available upon request during audits.
- B. Before access authorization is granted allowing third party vendors, consultants, etc., to perform maintenance on equipment accessing KCJIS, including mobile computer devices, or service to the network accessing KCJIS a background check shall be conducted by the facility/parole office TAC or designee to prevent unauthorized access to KCJIS materials.
1. The check shall, at a minimum, include:
    - a. Locan name-based check for criminal history record information;
    - b. State and Federal check for criminal history records information; and
    - c. Local, State and Federal warrant check.
  2. An Awareness Statement shall be in place prior to staff from any other criminal justice agency/company (i.e., vendors) being allowed access to the network accessing KCJIS.
- C. Any LAN connected to the secured KCJIS network shall have only one secured access point to or from the LAN; that being the router connection to the secured KCJIS network with other outside connections.
1. All routers, modems, CSU's/DSU's, and servers on the secured KCJIS network shall be placed in a secure facility location at all times as approved by the Network Security OfficerEnterprise IT Security Officer.
  2. Any closed LAN, open LAN or MAN shall be connected to a firewall before connecting to the router. See Attachment C, Network Architecture Diagram.

- D. Traffic from the KDOC on the KCJIS network shall be for criminal justice business purposes only.
  - 1. Facility/parole office TACs shall ensure that all traffic from the Kansas Department of Corrections on the KCJIS network shall be for criminal justice business purposes only (see Section II.).
- E. All backups or other copies of KCJIS information shall be protected to preclude unauthorized access to the data when removed from the secured physical location.
  - 1. The programs and procedures for ensuring adequate protection shall have been approved by the NSOESO.
  - 2. Any information removed from the secured physical location shall be logged and the log retained for a period of three (3) years by the facility/parole office.
- F. No modems shall be permanently connected to any LAN on the KCJIS network.
  - 1. Temporary and controlled modem connections are permitted only if the modem is enabled during the time the dial-in is necessary and immediately disabled.
  - 2. No dial-in modems shall be permanently connected to any LAN or PC on the secured KCJIS network.
    - a. Permanently connected means a modem that is connected and is never disabled at any time.
    - b. Temporary and controlled modem connections are permitted only when the modem is enabled during the time that the dial-in was necessary and immediately disabled.
    - c. No modems shall be connected to a LAN on the secured KCJIS network for dial-in access unless the modem is only enabled during the time the dial-in was necessary and immediately disabled after access.
  - 3. Direct dial-in access to a workstation is not permitted.
    - a. Dial-in to a RAS at a regional MAN is permitted.
  - 4. Requests for dial-out capabilities to be used to establish added network connections shall be made in advance in writing to the NSOESO.
- G. Any remote office connected to a regional MAN will not require a firewall between the office and the MAN.
- H. Technical staff shall comply with all components of this policy.
  - 1. Failure to comply shall be grounds for termination, regardless of intent.

## **V. Training Policies**

- A. All personnel shall be trained, within six (6) months of election, selection or assignment, on privacy and security issues regarding the use of the information.
  - 1. Once trained, all personnel shall sign an Awareness Statement, Attachment B (Form #05-172-001), acknowledging that they understand the penalties and/or circumstances constituting the misuse of this information and filed in accordance with paragraph V.A.2.
  - 2. The facility/parole office TAC shall retain the statements.
  - 3. The statements shall be provided upon request during audits.

4. The facility/parole office TAC shall maintain complete documentation of all training received.
  5. Training documentation shall be provided upon request during audits.
- B. Within six (6) months of election, selection or assignment, criminal justice administrators and personnel who supervise employees who either use workstations accessing KCJIS or have access to KCJIS information, shall obtain training concerning capabilities of the KCJIS network, regulations, policy, audit requirements, sanctions, and related civil liability risks.
1. The facility/parole office TAC shall maintain complete documentation of all training received.
  2. Training documentation shall be provided upon request during audits.
  3. Records of this training shall be kept in the security audit log.
- C. All KCJIS workstation users and agency technical support personnel shall be provided network security awareness training within six (6) months of their employment or assignment.
1. The facility/parole office TAC shall maintain complete documentation of all training received.
  2. Training documentation shall be provided upon request during audits.
- D. All KCJIS workstation users shall be trained to their level of access within six (6) months of employment or assignment.
1. All NCIC full access operators shall pass the NCIC certification test given by the Kansas Highway Patrol.
    - a. This certification shall be renewed every two (2) years.
    - b. The facility/parole office TAC shall maintain a record of all NCIC certifications by operator name and certification date.
    - c. If the certification expires, the operator shall not be allowed on the network until re-certification is completed.
  2. The employing agency or the KHP shall certify all NCIC less than full access operators.
    - a. This certification shall be renewed every two years.
    - b. All facility/parole office certification programs shall be submitted to the Agency TAC for review and approval.
    - c. NCIC Less than full access operators shall pass a test instrument approved by the KHP.
      - (1) Instructors for the NCIC less than full access operator certification program shall maintain a current NCIC full access operator certification and shall have successfully completed, at a minimum, training of trainers for part-time trainers.
    - d. The facility/parole office TAC shall maintain complete documentation of all training provided.
    - e. Training documentation shall be provided upon request during audits.

- f. Annually, either on or the first work day following July 1<sup>st</sup>, a list of all less than full access operators and the dates of their certifications will be provided to the Agency TAC for furtherance to the CTO.
- 3. All MDT users shall be trained on the unique use of mobile computer access, its limitations and physical security.
  - a. Lessons plans for this training must be approved in advance by the Agency TAC.
  - b. The facility/parole office TAC shall maintain complete documentation of all training provided.
  - c. Training documentation shall be provided upon request during audits.
- E. All KCJIS non-workstation users with the need to access NCIC information (referred to as practitioners) shall receive training in accordance with their assigned duties as described below:
  - 1. All law enforcement officers, within six (6) months of employment or assignment, shall receive basic training on NCIC matters adhering to the minimum curriculum recommended by NCIC to ensure effective use of the system and compliance with NCIC policies and regulations.
    - a. Law enforcement personnel are defined by NCIC to include corrections officers and parole officers.
    - b. The facility/parole office TAC shall maintain complete documentation of all training received.
    - c. Training documentation shall be provided upon request during audits.
  - 2. All other criminal justice employees, such as records clerks and attorneys, shall receive appropriate training within six (6) months of employment or assignment.
    - a. The facility/parole office TAC shall maintain complete documentation of all training received.
    - b. Training documentation shall be provided upon request during audits.
- F. All training in CJIS/KCJIS/NCIC shall be approved in advance and in writing by the Agency TAC.
- G. All training taught by KDOC personnel shall include written lesson plans, course objectives, and instructor evaluations that shall be filed with the facility/parole office staff development unit.
- H. All training taught by non-KDOC personnel shall include an outline, agenda or other items to describe the training issues covered that shall be filed with the facility/parole office staff development unit.

## **VI. Administrative Security Policies**

- A. Each facility/parole office with KCJIS access is responsible for their records keeping practices.
- B. Facility/Parole office record keeping practices will be monitored through compliance audits.
- C. All information received from the KCJIS Network shall be destroyed when no longer needed.
  - 1. This includes information stored on discs and workstations.
- D. Documentation that supports any operation on the KCJIS Network, training personnel, security violations, etc., shall be provided to authorized audit staff upon request.

- E. The Secretary of Corrections shall appoint an Agency TAC who shall serve as the primary point of contact between the CTA/CTO/KBI/KHP and departmental facilities and parole offices. Responsibilities of the Agency TAC include:
1. Act as the primary liaison between the Department and NCIC, KBI, and KHP
  2. Monitor the security of all CJIS relation information and workstations supported by the Department. This includes, but is not limited to:
    - a. Maintaining accurate user information
    - b. Performing security measures relating to the application of LINXX security software
    - c. Overseeing proper backup measures; and,
    - d. Enforcing and implementing network security policies
  3. Update user agreements
  4. Assist KHP and NCIC during department-wide audits
  5. Coordinate training of all operators
  6. Maintain and update user documentation throughout the agency
  7. Understand the record system and communications
  8. Properly handle NCIC, NLETS, KCJIS, KBI, and KHP information; and,
  9. 9. Other responsibilities as directed by the CJIS governance organization
  10. Approve all KCJIS node/equipment/software additions, deletions, and modifications
- F. If a violation of security is discovered, the discovering facility/parole office shall notify the Agency TAC without delay using the guidelines outlined in Section III. Physical Security Policies.
1. The Agency TAC shall notify the KCJIS Security Officer without delay and within one (1) business day.

## **VII. Network Security Sanctions**

- A. The Kansas Department of Corrections facilities/parole offices shall secure their site and any equipment accessing KCJIS from unauthorized access.
1. The programs and procedures for ensuring security shall have been approved by the Network Security OfficerEnterprise IT Security Officer.
- B. Failure to successfully address agency security requirements may be seen by the KCJIS Security Officer as grounds for revocation of access to the KCJIS network.
1. Should access to the KCJIS network be revoked or terminated at any facility/parole office for security reasons;
  2. The facility/parole office TAC shall document, in writing, what steps have been taken to secure the site;
  3. This document shall be sent first to the Agency TAC for review and approval;

4. Upon approval, the Agency TAC shall forward the document to the CJIS Security Officer and the KCJIS Unit.
5. If the CJIS Security Officer determines that the agency security requirements have not been successfully addressed, that determination may be appealed to the NCIC Control Terminal Officer.
  - a. Appeals to the NCIC Control Terminal Officer shall be made through the Agency TAC.

## **VIII. Audit Policy**

- A. Periodically, the KBI and/or the KHP will conduct audits to assure compliance with established policies.
  1. The following areas may be reviewed during on site audits:
    - a. Network Security;
    - b. Personnel Security;
    - c. Physical Security;
    - d. Technical Security;
    - e. Training Issues;
    - f. Administrative Security;
    - g. Information Quality;
    - h. Dissemination;
    - i. Validation Review;
    - j. NCIC Quality Assurance; and/or,
    - k. Kansas Hot Files Quality Assurance.
- B. Should a facility/parole office receive a final audit report noting any area of noncompliance, the facility/parole office administrator shall respond in writing within 25 days to the Agency TAC.
  1. The Agency TAC shall forward a copy of the facility/parole office response to the NCIC CTO or designee.

**NOTE:** The policy and procedures set forth herein are intended to establish directives and guidelines for staff and offenders and those entities that are contractually bound to adhere to them. They are not intended to establish State created liberty interests for employees or offenders, or an independent duty owed by the Department of Corrections to employees, offenders, or third parties. Similarly, those references to the standards of various accrediting entities as may be contained within this document are included solely to manifest the commonality of purpose and direction as shared by the content of the document and the content of the referenced standards. Any such references within this document neither imply accredited status by a Departmental facility or organizational unit, nor indicate compliance with the standards so cited. The policy and procedures contained within this document are intended to be compliant with all applicable statutes and/or regulatory requirements of the Federal Government and the state of Kansas. This policy and procedure is not intended to establish or create new constitutional rights or to enlarge or expand upon existing constitutional rights or duties.

## **REPORTS REQUIRED**

<u>Name/Type of Report</u>	<u>By Whom/To Whom</u>	<u>Due</u>
Less Than Full Access Operators List w/Certification Dates	Facility/Parole Office TAC to Agency TAC	July 1 or the following work day

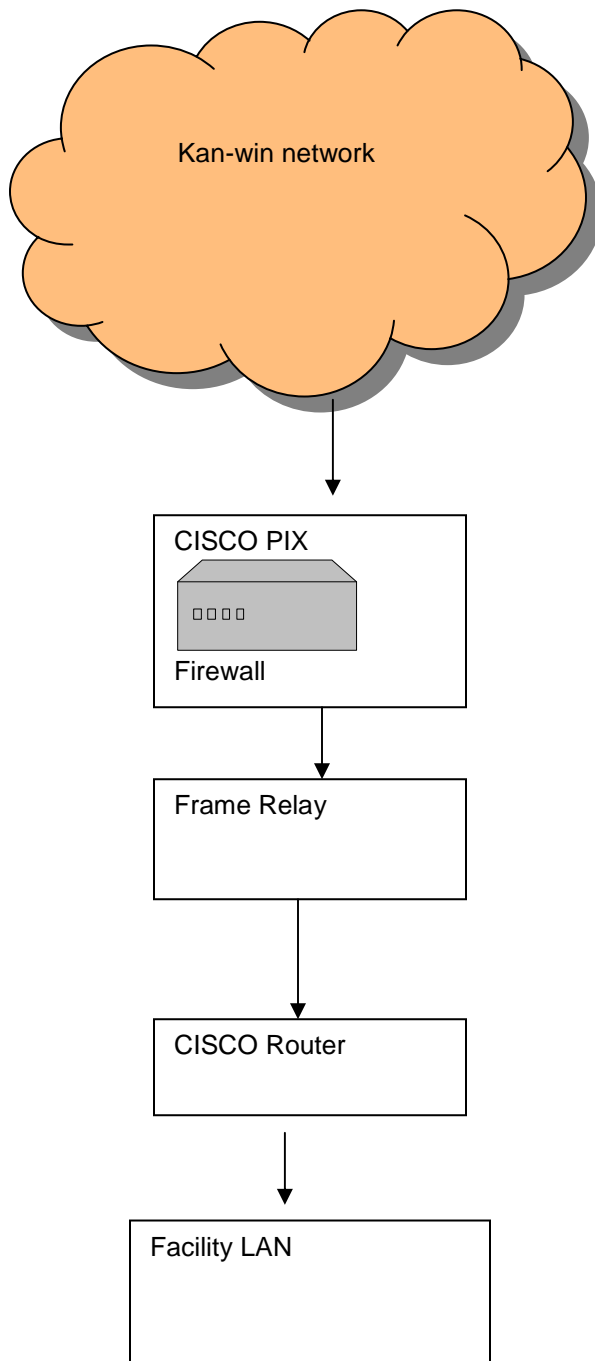
## **REFERENCES**

KSA 21-3902, 22-4701, 38-1501 et seq., 38-1601 et seq.  
IMPP 05-101

## **ATTACHMENTS**

Attachment A – Network Schematic, 1 page  
Attachment B – KDOC Employees Awareness Statement, 2 pages  
Attachment C – KDOC Network Architecture, 1 page  
Attachment C – KDOC Network Architecture, 1 page

## NETWORK SCHEMATIC



**Kansas Department of Corrections**

**USER NETWORK AND COMMUNICATIONS AWARENESS STATEMENT**  
**EMPLOYEES AWARENESS STATEMENT**

(Including full-time, part-time, temporary, contract personnel and volunteers)

Date:

To: Appointing Authority

Facility / Office: \_\_\_\_\_

From:

I have read, understand and agree to comply with all provisions of IMPP 05-131: *Platform Usage and Administration*, IMPP 05-145: *Systems Administration* and IMPP 05-171: *Information Systems Security*. I understand that all movement on the Electronic Network is tracked by DISC and available to DOC. I understand that the Electronic Network is a tool provided only to assist me in performing my job. I understand that this technology is provided for official state business only. Inappropriate use (including but not limited to the e-mail system and the Internet) may result in monitoring. Inappropriate use may result in the proposal of disciplinary action up to and including termination of employment in accordance with K.S.A. 75-2949(a)(3) and other appropriate statutes. System-wide checks will be conducted on a periodic basis to assure that inappropriate sites are not being utilized. Internet/e-mail activity of an inappropriate nature that is substantiated may result in the proposal of disciplinary action. I understand that the Internet lines are not secure; therefore, confidential / restricted Departmental information not specifically approved for release through the Internet shall not be transmitted over the Internet.

Access to criminal history record information, such as defined in K.S.A. 22-4701 et. Seq., and use and dissemination of such information is governed by state and federal laws and regulations, particularly the federal regulations on criminal justice information systems, 28CFR Part 20.25, also referred to as "Title 28". Similarly, juvenile justice information is controlled by the provisions of the Child in Need of Care Code and the Juvenile Offender Code, as defined by K.S.A. 38-1501, et. Seq. and K.S.A. 38-1601 et. Seq.

Criminal history information is releasable to criminal justice agencies requesting such information for criminal justice purposes. Juvenile offender history is also available for criminal justice purposes.

Title 28 states, "that any agency or individual violating subpart B of these regulations, shall be subject to a fine not to exceed \$10,000". Kansas law also provides specific criminal penalties for unlawfully accessing or disseminating criminal history information.

K.S. A. 22-4707 (d) provides:

"...Any individual violating or causing a violation of the provisions of this section shall be deemed guilty of a class A misdemeanor...a conviction shall constitute good cause to terminate employment..."

Pursuant to Kansas Statutes enacted in Chapter 184 of the 1995 session laws:

K.S.A. 21-3902 (a) (3) describes the following act as official misconduct:

“...Using confidential information acquired in the course of and related to the officer’s or employee’s office or employment for private benefit or gain of the officer or employee or another or to maliciously cause harm to another...”

K.S.A. 21-3902 (c)(1) and (c)(4) defines:

This act as a class A nonperson misdemeanor, and upon conviction mandates that a public officer or employee shall forfeit such officers or employee’s office or employment.

As an employee of the Kansas Department of Corrections you may have the right to access, view, use, and/or disseminate criminal and/or juvenile history record information, and other official documents, such as investigative case files, intelligence data, driver license information, vehicle registration, etc. However, the use of this information must be necessary to complete work assignments or for the proper dissemination. This information cannot be obtained for a personal desire to know or to inform or provide others outside of the criminal justice system with information. Misuse of this protected information in this or a similar manner may subject you to civil and criminal penalties and/or fines, and may be considered grounds for suspension, demotion, dismissal, or other adverse action.

If I am responsible for computers that are accessible to inmates I will take all necessary safeguards to ensure the following:

Inmate computers are not connected to the KDOC network unless approved by the local network administrator. Any modifications to an inmate’s computer must be approved by the local network administrator prior to the changes being made. A current inventory of software and hardware must be provided to the local network administrator and updated at least once a year.

The Kansas Department of Corrections agrees to provide training in the area of proper dissemination of criminal history and related data.

*My signature below certifies that I have read and will comply with the above.*

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Supervisor Signature

\_\_\_\_\_  
Date

## KDOC NETWORK ARCHITECTURE

